Response to the Government's Call for Views:
Proposals for Regulating Consumer Smart Product Cyber Security

Submitted by
Prof. Derek McAuley **derek.mcauley@nottingham.ac.uk**
Dr. Hamed Haddadi **h.haddadi@imperial.ac.uk**
Dr. Lachlan Urquhart **lachlan.urquhart@ed.ac.uk**
Dr. Jiahong Chen **jiahong.chen@nottingham.ac.uk**

3 September 2020

Defence Against Dark Artefacts (DADA) is an EPSRC-funded research project, addressing the home network security issues with a focus on the acceptability and usability challenges from the perspective of end-users.

Prof. McAuley is Professor of Digital Economy, Director of Horizon Digital Economy Research (University of Nottingham) and Principal Investigator of DADA.

Dr. Haddadi is Reader in Human-Centred Systems (Imperial College London) and Co-Investigator of DADA.

Dr. Lachlan Urquhart is Lecturer in Technology Law (University of Edinburgh) and Researcher Co-Investigator of DADA.

Dr. Chen is Research Fellow in IT Law (University of Nottingham) and Postdoctoral Researcher of DADA.

Proposals for Regulating Consumer Smart Product Cyber Security - Call for Views July 2020

Feedback Form

The questions set out below seek your feedback on the government's Call for Views on proposals for improving the cyber security of consumer smart products sold in the UK through legislation.

Respondents are encouraged to provide answers to these questions using the feedback survey for this Call for Views. Alternatively, if unable to complete the survey, respondents can download and populate this feedback template and email their responses directly to securebydesign@dcms.gov.uk.

We recommend reading the Call for Views in full before submitting feedback. You do not have to answer all of the questions. All responses should be submitted in advance of the closing date for this Call for Views, which is **23:59 Sunday 6th September 2020**.

Privacy notice

The following is to explain your rights and give you the information you are entitled to under the Data Protection Act 2018 and the General Data Protection Regulation ("the Data Protection Legislation"). This notice only refers to your personal data (e.g. your name, email address, and anything that could be used to identify you personally) not the content of your response.

1 - The identity of the data controller and contact details of our Data Protection Officer

The Department for Digital, Culture, Media and Sport ("DCMS") is the data controller. The Data Protection Officer can be contacted at dcmsdataprotection@dcms.gov.uk.You can visit the DCMS website to find out more about how DCMS uses and protects your information.

2 - Why your personal data is being collected

Your personal data is being collected as an essential part of the Call for Views process, so that the government can contact you regarding your response and for statistical purposes, such as to ensure individuals cannot complete the survey more than once.

3 - The legal basis for processing personal data

The Data Protection Legislation states that, as a government department, the department may process personal data as necessary for the effective performance of a task carried out in the public interest. i.e. a Call for Views.

4 - How your personal data will be shared

Copies of responses may be published after the survey closes. If this happens, the government will ensure that neither you nor the organisation you represent are identifiable, and any response used to illustrate findings will be anonymised.

If you want the information that you provide to be treated as confidential, please contact foi@dcms.gov.uk. Please be aware that, under the Freedom of Information Act (FOIA), there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain why you regard the information you have provided as confidential. If the

government receives a request for disclosure of the information, the government will take full account of your explanation, but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

5 - How long your personal data will be kept for

Your personal data will be held for two years after the survey is closed. This is so that the department is able to contact you regarding the result of the survey following analysis of the responses.

6 - Your rights in relation to access, rectification and erasure of data

The data that is being collected is your personal data, and you have considerable say over what happens to it. You have the right:

- *to see what data we have about you:*
- *to ask us to stop using your data, but keep it on record;*
- *to have all or some of your data deleted or corrected;*
- *to lodge a complaint with the independent Information Commissioner if you think we are not handling your data fairly or in accordance with the law.*

You can contact the ICO at https://ico.org.uk/, or telephone 0303 123 1113. ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

7 - Additional information

Further to the above, you should also be aware of the following:

- *Your personal data will not be sent overseas.*
- *Your personal data will not be used for any automated decision making.*
- *Your personal data will be stored in a secure government IT system.*

If you need any further information related to the processing of your personal data please contact the DCMS Data Protection Team at dcmsdataprotection@dcms.gov.uk and specify which survey you have concerns about.

Privacy Notice and Confirmation of Consent

Please confirm that you have read and understood the Privacy notice, and consent to participating in the Call for Views.	
Please confirm by entering "x" in the box below	
Confirmation of Consent:	x

Demographic questions

1) Are you responding as an individual or on behalf of an organisation?	
*Please indicate your response by entering "x" in **one** of the boxes below*	
Individual	x
Organisation	

2) [if individual] Which of the following statements best describes you?	
*Please indicate your response by entering "x" in **one** of the boxes below*	
Cyber security professional	
Employer/employed in the consumer goods sector	
Professional in another sector	
Public sector official	
Academic	x
Interested member of the general public	
Other (please specify in the box below)	

3) [if organisation] Which of the following statements best describes your organisation?	
*Please indicate your response by entering "x" in **all boxes that apply***	
Producer of consumer smart products	
Distributor of consumer smart products	
Cyber security provider	
An academic or educational institution	
A trade body representing "Producers"	
A trade body representing "Distributors"	
Other (please specify in the box below)	

4) [if organisation] Which of the following statements best describes your organisation?	
Note that this information will be used to enable a view of how these proposals will impact businesses based in different countries in the UK, as well as those based outside of the UK. *Please indicate your response by entering "x" in **one** of the boxes below*	
UK only based organisation	
Multinational organisation based in the UK	
Multinational organisation based in an EU country outside of the UK, which operates in the UK	
Multinational organisation based in a non-EU country outside of the UK, which operates in the UK	
Other (please specify in the box below)	
[if organisation] Which country is your organisation's head office based in? *Please type your answer into the box below*	

5) [if organisation] Which of the following statements best describes your organisation?	
*Please indicate your response by entering "x" in **one** of the boxes below*	
Cyber security	
Production / Manufacturing	
Distributor / Wholesale / Retail	
Telecoms providers	
Information & communication technology (ICT)	
Health	
Critical National Infrastructure and National Security (please specify sector in the box below)	
Transport & Storage (including postal)	
Finance & Insurance	
Property	

Construction	
Business administration & support services	
Education / Academia	
Public administration & defence	
Arts, entertainment, recreation	
Agriculture, forestry & fishing	
Civil society	
Accommodation & food services	
Other services (please specify in the box below)	

6) [if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.	
*Please indicate your response by entering "x" in **one** of the boxes below*	
Less than 10 people	
10-49	
50-249	
250-999	
1,000 or more	

7) [if organisation] What is the name of the organisation you are responding on behalf of?
Please type your answer into the box below

8) Are you happy to be contacted to discuss your response and supporting evidence?	
*Please indicate your response by entering "x" in **one** of the boxes below*	
Yes	x
No	

9) [if organisation and yes to 8] Please provide a contact name and email address below:
Please type your name in the box below
Please type your email address in the box below

Scope of regulation questions

10) To what extent do you agree or disagree that the following categories of conventional IT devices should be included within the scope of the proposed regulation?					
Please indicate your response by entering "x" into the column that best represents your view in each of the three rows					
	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
Laptops					x
PCs					x
Smartphones					x
Please explain the reasons for your answers to the above question by typing your answer into the text box below					
Laptops	Like smart products, conventional IT devices are also subject to cybersecurity threats to individual users and the network, and thus, there is no reason they should be excluded from the scope of the proposed regulation. In fact, due to the higher level of versatility, connectivity and computational and storage capacity, they tend to involve a higher level of risks and should be placed under an even stricter regime (e.g. subject to all 13 principles) as a consideration for future regulatory initiatives. Also, while the proposal differentiates consumer smart products from industrial ones, this distinction is not always straightforward for conventional IT devices due to their generic functionalities and the increasing blurred lines between home and workplaces.				
PCs	Same as above.				
Smartphones	Same as above.				

11) The ambition of this regulation is to establish a robust baseline across all smart connected products and to protect consumers and the wider economy from a range of harms. Please detail any unintended impacts that this proposed regulation would have, beyond the ambition stated above, to your organisation / the wider economy.	
Please think about our proposed definitions of "Producers", "Distributors" and any other organisations in the consumer smart product supply chain when answering this question. Please clearly state which types of organisation you are referring to in your response. *Please type your answer into the boxes below:*	
Producers	N/A
Distributors	N/A
Other organisations (please specify)	N/A

Wider economy	Potential positive impact: Create a boost for the cybersecurity sector; promote trust and adoption of smart technologies among consumers; and enhance the reputation and competitiveness of British smart products in the global market. Potential negative impact: Increase compliance costs, which could potentially be shifted to consumers.

12) Please share your views on the suggested supplementary guidance to help businesses to implement the proposed security requirements (provided in section 4 - Obligations of the Call for Views). Are there any other forms of guidance you feel should be included?
Please type your answer into the box below
It should be considered to empower the designated regulator to maintain a list of accredited, trusted and independent third-parties who can test the products, as a standard manner for producers to acquire assurance and for distributors to perform the duty of care. This would also incentivise vulnerability reporting from manufacturers to testers.

13) The proposed approach suggests using a broad definition of network-connectable product classes which could be in scope and specifying specific categories of products that are out of scope. Do you agree or disagree with this suggested approach?	
*Please indicate your response by entering "x" in **one** of the boxes below*	
Agree	x
Disagree (please explain in the box below)	
Don't know	
*Please share any views that you have on **alternative wording, approaches**, or **ways to improve the proposed approach** of using a broad definition of network-connectable product classes which could be in scope and specifying specific categories of products that are out of scope.* *Please type your answer into the boxes below:*	

Security requirements feedback

14) Please outline any further feedback on the security requirements, as set out in section 3.3 of the Call for Views.	
Please type your answer into the boxes below:	
Security requirement 1 - Ban universal default passwords	On the one hand, password is not always a suitable authentication method for all types of smart products, and on the other, regulating only password mechanisms may create an incentive for producers to opt for less effective methods. As such, a catch-all clause should provide that where password authentication is not available, alternative methods should be put in place to ensure a same level of security. The Government should also consider supporting further research into alternatives mechanisms that are more effective and usable to end-users.
Security requirement 2 - Implement a means to manage reports of vulnerabilities (providing a publicly available vulnerability disclosure policy which includes at least contact information for the reporting of issues, and information on timelines for initial acknowledgement of receipt and status updates until the resolution of the reported issues)	No response.
Security requirement 3 - Provide transparency on for how long, at a minimum, the products will receive security updates	There are technological solutions being developed to support end-users of smart products to manage security risks, but this would depend on information provided by manufacturers in standardised formats. In this regard, we suggest that, in addition to the "accessible" and "clear and transparent" elements, Requirement 3 should also mandate "where technically possible, in a machine-readable and interoperable manner". One possible approach, for example, is to require the disclosure of information on whether a product is being supported with Manufacturer Usage Description Specification,[1] so local network management systems can support the user accordingly. We welcome the latest proposal's identification of potential ways to manage cybersecurity risks for end-of-life smart products, but call for further clarification on the nature of such suggestions (statutory obligations / code of practice requirement / recommended best practices) in a later version.

[1] https://www.rfc-editor.org/rfc/inline-errata/rfc8520.html, see sec 3.6.

Obligations questions

15) This proposal requires an exchange of information between “Producers” and “Distributors” in the supply chain to confirm compliance.

4.2 - Box 6 - Draft proposal and example guidance content for “Producer" obligations

“A prohibition on a “Producer” from supplying or making a product within scope available in the UK market unless the product is compliant with the security requirements.”

This places an obligation solely on “Producers” to evidence compliance with the security requirements to the “Distributors”. Should this information exchange approach, as set out in box 6 of the Call for Views, be adopted?

*Please indicate your response by entering “x” in **one** of the boxes below*

Yes	x
No (please explain in the box below)	
Don’t know	

Should “Distributors” also have obligations as part of this information exchange?

*Please indicate your response by entering “x” in **one** of the boxes below*

Yes	x
No (please explain in the box below)	

Distributors should also make such information available to consumers at the point of sales, so as to avoid consumers having to find such information only after opening the package.

Don't know	

16) The proposed approach intends to include entities who supply or make smart products available online, e.g. those who act as a marketplace, a platform for consumer sales online or provide either first or third party sales.

Do you agree or disagree with this approach?

*Please indicate your response by entering "x" in **one** of the boxes below*

Agree (please explain in the box below)	x
Online marketplaces / platforms are best-positioned to communicate compliance information to consumers and verify producers and distributors' obligations are fulfilled. There should also be a statutory obligation for these platforms to disclose the required information at the point of purchase in an accessible way.	
Disagree (please explain in the box below)	
Don't know	

17) Should the definitions such as "Producer" and "Distributor" (see box 5 and 7 in the Call for Views) in existing product safety regulations (such as the Radio Equipment Regulations 2017, and the General Product Safety Regulations 2005) be used as a basis for the definitions in this proposal?

"Producer" in the working definition means;

1. *the **manufacturer** of a product, when they are established in the UK and any other person presenting themself as the manufacturer by affixing to the product their name, trade mark or other distinctive mark, or the person who reconditions the product;*
2. *when the manufacturer is not established in UK*
   - *if they have a **representative established in the UK**, the representative,*
   - *in any other case, the **importer** of the product from outside the UK into the UK (which in some cases can be a retailer).*

"Distributor" means any person in the supply chain, other than the manufacturer, authorised representative or the importer, who makes [a product] available on the market

Note that this proposal would also place obligations on "Distributors" who act as a marketplace or a platform for consumer sales online.

*Please indicate your response by entering "x" in **one** of the boxes below*

Yes	x
No (please provide details of any alternative approaches that could be considered in the box below)	
Don't know	

Enforcement approach questions

18) Box 10 in the Call for Views describes a suite of example corrective measures and sanctions which could be made available to the enforcement body in the event of non-compliance. These are listed below (see box 10 in the Call for Views for further details):

- **Voluntary and Corrective Measures**
- **Compliance Notice**
- **Undertaking**
- **Enforcement Order**
- **Security Notice**
- **Forfeiture & Destruction**
- **Administrative Penalties**
- **Financial Penalty**

Is the proposed suite of corrective measures and sanctions proportionate overall?

*Please indicate your response by entering "x" in **one** of the boxes below*

Yes	x
No (please explain in the box below)	
Don't know	

Are each of the potential measures below an effective response or deterrent to non-compliance?

Please indicate your response by entering "x" into the column that best represents your view in each of the eight rows, explaining why in instances where you have selected "no".

Potential measures	Are the potential measures effective?		If no, please explain
	Yes	No	
Voluntary and Corrective Measures		x	The investigatory power should explicitly include the power to require technical information on how the requirements are met. As stated in our previous response,[2] we remain of the view that such powers are already being exercised by Trading Standards under the Consumer Rights Act 2015 and therefore they would be a suitable candidate enforcer.
Compliance Notice	x		
Undertaking	x		
Enforcement Order	x		
Security Notice	x		

[2] https://nottingham-repository.worktribe.com/output/3909097

Forfeiture & Destruction	x		
Administrative Penalty	x		
Financial Penalty	x		

19) Are there significant barriers that would prevent your organisation from becoming compliant with the security requirements within the suggested timescales (see box 9 of the Call for Views and summarised below)?

Security requirement 1 - Ban universal default passwords - **9 months**

Security requirement 2 - Implement a means to manage reports of vulnerabilities (providing a publicly available vulnerability disclosure policy which includes at least contact information for the reporting of issues, and information on timelines for initial acknowledgement of receipt and status updates until the resolution of the reported issues) **- 3 months**

Security requirement 3 - Provide transparency on for how long, at a minimum, the product will receive security updates **- 6 months**

Please indicate your response by entering "x" into the column that best represents your view in each of the three rows.

For rows where you have selected Yes, what are the barriers for implementation to the suggested timescales, how much time would be required for your organisation to become compliant with the security requirements (in months) and how could these barriers be mitigated?

Please type your answer into the relevant boxes below

security requirement	**Are there significant barriers?**			**Details of barriers (if yes only)**		
	Yes	No	Don't Know	Barriers for implementation (if yes only)	How long it would take to become compliant (if yes only - months)	How barriers could be mitigated (if yes only)
Security requirement 1 Ban universal default passwords						
Security requirement 2 Implement a means to manage reports of vulnerabilities						
Security requirement 3 Provide transparency on for how long, at a minimum, the products will receive security update						

20) Please provide details of any additional costs to your organisation that would result from implementing each of the security requirements in our proposed approach

If your organisation is both a "Producer" and "Distributor" of consumer smart products, please indicate explicitly which aspect of your organisation's operations these costs would impact on in your answers.

Please also indicate whether these costs would be one-off costs or incurred annually. Please type your answers into the appropriate boxes below:

Security requirement	Description of additional costs	Job roles involved and number of hours required per job role	Estimated total cost per product line (£)	Estimated total **annual** cost to your organisation (£)
Security requirement 1 Ban universal default passwords				
Security requirement 2 Implement a means to manage reports of vulnerabilities				
Security requirement 3 Provide transparency on for how long, at a minimum, the products will receive security update				

Please provide details of any benefits to your organisation that would result from the implementation of these security requirements

Please type your response into the boxes below

Security requirement	Description of benefits
Security requirement 1 Ban universal default passwords	
Security requirement 2 Implement a means to manage reports of vulnerabilities	
Security requirement 3 Provide transparency on for how long, at a minimum, the	

products will receive security update	

21) Please estimate any additional reporting costs to your organisation				
When answering this question, where possible, please clearly describe any costs, including job roles, the estimated number of hours of staff time associated with each job role, total cost estimates per product line (specifying whether one-off or annual), and overall total annual cost to your organisation. *Please type your response into the boxes below*				
Reporting variant	Description of costs	Job role involved and number of hours required per job role	Estimated total cost per product line (£)	Estimated total **annual** cost (£)
The proposed obligation for "Producers" to demonstrate compliance with the security requirements to "Distributors"				
The requirement for "Distributors" to process information from "Producers"				
Are there any ways we could tailor our approach to mitigate these reporting impacts? *Please indicate your response by entering "x" in **one** of the boxes below*				
Yes (please explain in the box below)				
No				
Don't know				

22) To what extent do you agree or disagree with the criteria that would be considered for identifying an enforcement body, detailed in box 12 of the Call for Views and summarised below?

Example Considerations for designating an enforcement body

- scope and alignment of the proposed legislations with the relevant expertise of the enforcement body;
- approach used to regulate against non-compliance;
- capacity and resources available to the enforcement body to conduct enforcement activities;
- capabilities and skills of the enforcement body to conduct enforcement activity;
- existing relationships with the stakeholders who would be subject to the provisions of the legislation;
- future scope of the enforcement body to enforce additional security requirements;
- funding model used to operate the enforcement approach and its sustainability;
- monitoring and reporting capabilities.

And to what extent do you agree or disagree with the example powers for the enforcement body, detailed in box 13 of the Call for Views document and summarised below?

Example powers for the enforcement body

Although these are subject to change, the powers of the enforcement body could include, the:

- ability to fund testing in testing houses;
- ability to have a central reporting mechanism for use in instances where initial reports to the "Producer" have not resulted in action, or if products are identified from manufacturers that have no mechanism for vulnerability disclosure. This central reporting mechanism would enable security researchers, consumer groups, the general public and others, to report vulnerabilities in products within scope;
- capability to produce guidance materials for device compliance assessments to ensure compliance;
- ability to allocate an enforcement team with a responsibility of testing and monitoring products within scope;
- power to make a purchase of a product in order to test it or authorise an officer of the enforcement body to make a purchase of a device;
- ability for an officer of the enforcement body to enter and search any premises other than premises occupied only as a person's residence and inspect any record or device;
- ability to obtain and use search warrants and other such authorities;
- powers to prohibit the obstruction of officers and take action accordingly.

Please indicate your response by entering "x" into the column that best represents your view in each of the two rows

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
Box 12 - Example considerations for designating an enforcement body				x	
Box 13 - Example powers for the enforcement body				x	